EXHIBIT A

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

THE UNITED STATES OF AMERICA, Plaintiff, -against- ROMAN STORM, ET AL., Defendant.	Case No.: 23 Cr. 430 (KPF) Oral Argument: June 25, 2024

MEMORANDUM OF LAW IN SUPPORT OF ROMAN STORM'S MOTION TO DISMISS

Brian E. Klein
Keri Curtis Axel
Kevin M. Casey
Waymaker LLP
515 S. Flower Street, Suite 3500
Los Angeles, California 90071
(424) 652-7800

Attorneys for Roman Storm

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

I. PRELIMINARY STATEMENT

After obtaining political asylum in this country because of persecution in Russia and becoming passionate about cryptocurrency a few years later, defendant Roman Storm helped establish a U.S.-based company that raised significant money from respected venture capitalists and very publicly developed the open-source Tornado Cash protocol, which quickly became fully decentralized (*i.e.,* not in his, his company's or anyone else's control) and which provided a privacy solution for users of the widely-used Ethereum blockchain network. The government has wrongfully concluded that this conduct makes him guilty of multiple criminal conspiracy charges. But Mr. Storm is a developer, and his only agreement, together with the members of his U.S-based company, was to build software solutions to provide financial privacy to legitimate cryptocurrency users. This is not a crime.

The Indictment is fatally flawed and should be dismissed pursuant to Federal Rule of Criminal Procedure 12(b)(3)(v) for numerous legal reasons. Count One alleges a money laundering conspiracy, but by no stretch can Mr. Storm be deemed to have conspired to launder funds. Money laundering requires a "financial transaction" involving a "financial institution," yet Tornado Cash's publicly available protocol and the allegedly related software services, even as wrongfully characterized in the Indictment, do not conduct any financial transactions nor do they qualify as financial institutions as a matter of law. Moreover, the Indictment fails to allege facts that would show that Mr. Storm entered into a conspiratorial agreement with any bad actor to launder money, or that he had the specific intent to commit money laundering (nor could it). Indeed, the Indictment itself makes clear he could not have had such an agreement or such an intent because the Tornado Cash protocol was developed and became immutable before the alleged criminal conduct that is at the center of the money laundering count even occurred.

Count Two similarly fails in its attempt to allege a conspiracy to operate an unlicensed money transmitting business. By definition, Mr. Storm and his company did not operate a "money transmitting business" because, as is clear from the Indictment itself, users exerted full control over their funds. Further, the Second Circuit has made clear that a money transmitting business is one that charges a fee for transmitting funds, and the Indictment's allegations fail on this front too.

Count Three alleges a conspiracy to violate the International Emergency Economic Powers Act ("IEEPA"). Mr. Storm's alleged conspiratorial conduct regarding Tornado Cash falls squarely within the express exemption under IEEPA for the importation or exportation of "informational materials." Further, the Indictment fails to allege, as the IEEPA requires, that Mr. Storm acted willfully (nor could it). Again, by the time of the alleged sanctionable conduct, the Tornado Cash protocol was immutable and publicly available, and there was nothing Mr. Storm or anyone else could do to prevent a sanctioned entity from using it.

The Indictment also fails on several constitutional grounds. First, all three counts infringe Mr. Storm's First Amendment rights. It is well established that computer code is speech the First Amendment protects. Yet, all three counts here seek to criminalize the development and publication of code and the maintenance of a website that provided open-source software. To the extent the statutes at issue here can be used to criminalize such conduct, they violate the First Amendment, both facially and as applied. Second, the government's novel use of these statutes to criminalize such conduct also violates Mr. Storm's Due Process Clause right to fair warning. Insofar as the statutes could be stretched so far as to include the alleged conspiratorial conduct, they would be unconstitutionally vague because the statutes do not put the average citizen on notice that such conduct is proscribed. Finally, such a construction would necessarily

yield to the rule of lenity and to the principle that novel constructions that present constitutional problems should be avoided.

At its heart, this prosecution represents an unprecedented attempt to criminalize the development of software, which Mr. Storm and his colleagues had a First Amendment right to write, and which they freely and intentionally "opened sourced"—that is, published publicly without reserving intellectual property rights. There are no allegations that Mr. Storm conspired with any bad actors who later chose to use the software for their own illicit purposes (nor could there be); thus, as a matter of law, he cannot be held responsible for their conduct. The Court should dismiss the Indictment with prejudice.

II. RELEVANT BACKGROUND

A. Roman Storm[1]

Roman Storm has a lifelong love of technology and has never been afraid to stand up for freedom and justice—even at great personal cost.

Mr. Storm was born in Kazakhstan and, in 1996, following the collapse of the Soviet Union, he and his family relocated to Russia. His family was poor and conditions were difficult in the industrial city of Chelyabinsk where he grew up, but he earned good grades and admittance into a university, all the while developing a passion for computers and technology. While studying at South Ural State University, he became politically active and opposed Russia's invasion of Georgia, which eventually led to his persecution by the Russian Federal Security Service and other local agencies.

In 2008, he emigrated to the United States and the next year obtained political asylum.

[1] Mr. Storm provides this personal background for the Court's general understanding of the events leading up to the Indictment in this case. The dispositive facts for purposes of this motion are, of course, those contained in the Indictment, which are discussed in the sections that follow.

As a newly arrived immigrant appreciative of the opportunities afforded in this country, Mr. Storm rebuilt his life from scratch, working low-wage jobs while taking computer science courses at the City College of San Francisco. He was always drawn to the tech industry and the innovative environment of Silicon Valley, and he has held multiple IT jobs at various well-respected technology companies, including Amazon.

In or around 2014, Mr. Storm learned about Bitcoin, a then-nascent cryptocurrency based on blockchain technology. Fascinated with the promise of this technology and viewing it as a programmable form of digital finance, he began investing in Bitcoin and attending blockchain conferences. His participation in such events exposed him to various blockchain projects, large and small, and he came to appreciate Ethereum, one of the most widely-used blockchain networks whose native cryptocurrency is ETH (Ether).

But he also learned that Ethereum had an issue that was preventing more widespread adoption and legitimate use. Specifically, transactions on the Ethereum blockchain are only pseudonymous, meaning that while the identity of whoever controls an Ethereum wallet address is not revealed on the blockchain, the complete transactional history of a given address is publicly available and stored and viewable forever as part of the blockchain's history. This creates significant privacy concerns for legitimate users that are not present if a person uses fiat currency, *e.g.,* a bank and U.S. dollars to engage in a transaction. For instance, an individual may want to donate ETH to a political cause without exposing themselves to potential harassment by the cause's opponents (*e.g.,* a Russian donating to a Ukrainian charity). As another example, an individual holding significant amounts of cryptocurrency may not want that fact to be known, to shield themselves from scams or other attempts to defraud them.

Around 2014, Mr. Storm also learned of a cryptographic method called zero-knowledge proofs that had been incorporated into another well-known cryptocurrency, Zcash, and that could potentially act as a solution to the legitimate privacy concerns surrounding Ethereum, and a prominent industry leader encouraged him to develop one. Mr. Storm, together with his two co-founders, Roman Semenov (the other defendant in this case) and Alexey Pertsev (whom the Indictment refers to as a co-conspirator by calling him "CC-1"),[2] founded PepperSec Inc. ("Peppersec"), a Delaware-incorporated cybersecurity firm, initially to provide penetration testing, security assessments, and other "white hat hacker" services. Mr. Storm continued to pursue the idea of developing a potential privacy solution for Ethereum using zero-knowledge proofs. Eventually, MolochDAO, a decentralized autonomous organization that provides grants to support projects seeking to improve Ethereum, approached Peppersec to build a user interface for Semaphore, a privacy solution that MolochDAO was pursuing at the time. Mr. Storm, together with Mr. Semenov and Mr. Pertsev ("Peppersec developers"), agreed to build the interface, which eventually led to their interest in developing privacy-focused smart contracts on Ethereum, which became the Tornado Cash protocol.

B. Tornado Cash

The Indictment uses the defined term "Tornado Cash service" to refer to the Tornado Cash smart contracts, Peppersec's UI and website, and a "network of 'relayers' who provide customers with enhanced anonymity in exchange for a fee." (Ind. ¶¶ 9, 10.) The term "Tornado Cash service" is misleading because these components are separate and not parts of a unitary whole. The following is an explanation of certain components within the Tornado Cash universe that are relevant to the Indictment, starting with Ethereum.

[2] *See* Dkt. 1, Indictment ("Ind.") ¶ 2.

1. The Ethereum Blockchain

The Tornado Cash protocol (*i.e.,* its set of immutable smart contracts) operates on the Ethereum blockchain, a public ledger collectively hosted by the computers (or "nodes") that make up the Ethereum network. (*See* Ind. ¶¶ 4, 7.) Ethereum is one of the most widely used blockchains in the world and is publicly accessible through Internet-connected devices. Ethereum allows users to send and receive ETH (*Id.* ¶ 4), which is the second most used and valuable cryptocurrency after Bitcoin. ETH is stored in an Ethereum address, which is designated by a string of letters and numbers and is managed through wallets, which are in turn controlled by a private key known only to that user. (*Id.* ¶ 6.) All ETH transactions are publicly recorded on Ethereum. Because Ethereum is made up of numerous individual nodes, no single entity or person controls it. (Coin Center § 2.)[3]

Although the movement of ETH is traceable, the public ledger only identifies the sender and recipient by the string of letters and numbers that constitute an Ethereum address. (Ind. ¶ 7.) If, however, the identity of a particular individual *is* linked to a particular address (which can happen in many ways), the public nature of the blockchain means that any user can view the complete transactional history of that address—and, by extension, the associated individual. (Fed Primer at 122.)[4] This means the blockchain is pseudonymous not anonymous.

Ethereum also permits the use of smart contracts, which are open-source applications that any user can deploy to and interact with on the blockchain. (Ind. ¶ 8.) Once a smart contract is

[3] "Coin Center" refers to Alex Wae, Michael Lewellen, and Peter Van Valkenburgh, *How Does Tornado Cash Work?*, Coin Center, Aug. 25, 2022 (available at https://www.coincenter.org/education/advanced-topics/how-does-tornado-cash-work/).

[4] "Fed Primer" refers to Matthias Nadler and Fabian Schär, *Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers*, Federal Reserve Bank of St. Louis Review, Second Quarter 2023 (available at https://doi.org/10.20955/r.105.122-136).

deployed, it receives a unique address and can be viewed and used by any user without the need for an intermediary but, because smart contracts are, by default, "immutable," they cannot be removed or updated by anyone—even their creators—once they have been deployed. (Fed Primer at 124; Coin Center § 2.) In addition, because they are open-sourced, anyone can review the underlying code and deploy a similar—or even an identical—version. (Coin Center § 2.)

2. The Tornado Cash Smart Contracts

At the encouragement of other Ethereum users and developers, in August 2019, Peppersec developed and deployed a set of smart contracts, called Tornado Cash, which allow a user to transact privately on the Ethereum blockchain using zero-knowledge proofs. (Ind. ¶ 9; Coin Center § 3.) In short, the Tornado Cash smart contracts ("Tornado Cash") permit a user to deposit ETH and other Ethereum-based tokens to the smart contracts from one address and withdraw the same tokens to a different address without having any connection between the two addresses recorded on the blockchain. (Ind. ¶ 10.) Different Tornado Cash smart contracts permitted users to deposit different ETH amounts and, later, other cryptocurrencies. (*Id.* ¶¶ 10, 19.) These sets of smart contracts are referred to as "pools," according to the type and denomination of cryptocurrencies in a particular set of contracts. (*Id.* ¶ 17.) Users could interact with the various Tornado Cash pools directly or through an interface, such as a user interface ("UI") or Command Line Interface. A UI is a separate piece of software that can be run to assist a user with blockchain transactions by formulating requests that the user then sends to the protocol. Peppersec created a UI (*id*. ¶ 13), the codebase for which was open-sourced. In addition to Peppersec's UI, which is discussed in the Indictment, other developers created other

UIs and other applications to facilitate users' interactions with Tornado Cash.[5] Sophisticated blockchain users, however, can access the smart contracts without the need of any interface. (*Id.* ¶ 13.)

The Indictment's characterization of Tornado Cash as a "mixing service" is misleading: it is neither a currency mixer nor a service. (*See id.* ¶ 1.) Instead, "Tornado Cash" refers to a set of non-custodial smart contracts in which users maintain complete ownership and control over their assets without the need to rely on any service provider or other intermediary. (Coin Center § 3.) This is in stark contrast with custodial mixing services, which require a user to trust a service provider to take custody of the user's assets and provide the user's identifying information to retrieve equivalent (but not the same) cryptocurrency. (Fed Primer at 124.) Unlike users of such custodial services, Tornado Cash users never relinquish control of their assets to anyone, and they put in and retrieve their own assets. (Coin Center § 3.) Relatedly, although the "founders" never had any "private keys" to the Tornado Cash smart contracts, as the Indictment claims (Ind. ¶ 26), in May 2020, following a trusted setup ceremony, the smart contracts were updated to incorporate and finalize the contributions of over 1,000 community participants and to ensure no further changes could be made. (Coin Center § 3; Fed Primer at 127.) Put differently, by May 2020, the smart contracts were immutable, meaning no one, including Mr. Storm or the other Peppersec developers, could further modify or disable them. (*See* Ind. ¶ 26.)

3. Operation of Tornado Cash Pools

As a noncustodial protocol, the Tornado Cash smart contracts rely on zero-knowledge proofs, a cryptographic method in which one party can prove to another party that a given

[5] *See, e.g.*, BlockWallet, *On the Tornado Cash Situation* (Aug. 18, 2022), available at https://medium.com/blockwallet/on-the-tornado-cash-situation-6b95aafd9634 (explaining integration of Tornado Cash no longer supported after OFAC sanctions).

statement is true without conveying any additional information—including the statement itself. (Coin Center § 3.) To deposit tokens into a Tornado Cash pool, a user must first generate—locally, on the user's own computer—a deposit note, sometimes referred to as a "secret note," comprised of a long sequence of digits that is known only to the user. (*Id.* at 10; *see also* Ind. ¶ 15.) The user then applies a "hash," or encoded form of the deposit note, which the smart contract records in a public list (in its encoded form) of users' encoded deposit notes. (Coin Center § 3; *see also* Fed Primer at 127-28.) To be clear, neither Tornado Cash nor Peppersec created or stored the deposit note (or the "secret note," as the Indictment refers to it).[6]

To withdraw tokens, the user must first split their deposit note in two, with one side acting as a "secret" and the other as a "lock," both of which are then used to generate a zero-knowledge proof. (Coin Center § 3.) The user then supplies two inputs along with the request for a withdrawal: (1) a hash (or encoded form) of the lock; and (2) the zero-knowledge proof. (*Id.*) The smart contract uses this supplied information to verify that: (1) the tokens being withdrawn were previously deposited by someone; (2) the user initiating withdrawal is the same user who deposited the tokens; and (3) the tokens being withdrawn have not been previously withdrawn. (*Id.*) The Indictment claims that the Peppersec UI can, if utilized, "sen[d] the secret note to a smart contract . . . to initiate withdrawal" (Ind. ¶ 18), but this is incorrect. The Peppersec UI formulates the transaction requests the user needs to send the protocol, but the user

[6] The Indictment could be misread to suggest that Mr. Storm and his co-developers had access to the deposit note because it alleges that the Peppersec UI "would provide a unique secret note" to the user. (*See* Ind. ¶¶ 15, 19.) Elsewhere, though, the Indictment correctly acknowledges that the user "would be the only person with access to the secret note." (*Id.* ¶ 19.) To reiterate, Peppersec did not create the deposit note, and no one other than the user had access to it (unless the user chose to share it with someone else).

sends the request. (Int'l Academy at 12; 15-16.)[7] The UI does not maintain any record of any user's secret note. Once verified, the smart contract sends the user their tokens and records the encoded form of the lock on a public list of all users' encoded locks, to prevent the same tokens from being withdrawn again. (*Id.* at 12; *see also* Fed Primer at 128.)

A user may elect to use any interface, including the Peppersec UI, to assist in their interaction with the smart contracts. (Ind. ¶¶ 15-16.) But regardless of how the user interacts with the protocol, Tornado Cash operates in the same manner: the secret note, which is generated by the user on the user's computer and never publicly shared, acts as a cryptographic receipt for a user's deposit and allows the smart contract to verify, upon receiving a request for withdrawal, that the tokens being withdrawn were deposited by the same user and have not been previously withdrawn—all without revealing *which* user is withdrawing their deposit. Further, a user's deposited tokens are not "mixed" with other users' deposits, and users maintain complete control over their tokens, so long as they do not lose their secret note. If a secret note is lost, no one will be able to access the tokens associated with that deposit. (*See* Fed Primer at 127.)

4. Tornado Cash Relayers

Tornado Cash also gives users the option to withdraw their funds through the use of independent third-party operators known as "relayers." Because the smart contracts operate on Ethereum, every transaction requires the payment of a fee in ETH, known as a "gas" fee. (*See* Ind. ¶ 24.) Thus, to withdraw funds to a new wallet unassociated with the wallet used to deposit

[7] "Int'l Academy" refers to Benjamin Gruenstein, et al., *Secret Notes and Anonymous Coins: Examining FinCEN's 2019 Guidance on Money Transmitters in the Context of the Tornado Cash Indictment,* Working Paper 1, The International Academy of Financial Crime Litigators (Sept. 2023), available at https://edit.financialcrimelitigators.org/api/assets/b9fa10a1-5e91-4473-96f6-c240ff0761eb.pdf (analyzing FinCEN guidance and concluding that indictment here fails to state an offense because of lack of total independent control over funds).

the funds, a user would have to preload that new wallet with ETH to pay the gas fee for the withdrawal—but doing so could potentially compromise the anonymity of the user, because the transfer of the gas fee would be publicly recorded and traceable on the Ethereum blockchain. (*Id.* ¶ 25.) To address this issue, the Tornado Cash smart contracts permit a user to use a "relayer"—a third-party independent operator who runs a "relayer node"—to help execute the withdrawal of their funds by paying the gas associated with withdrawal transactions on the user's behalf, in exchange for an (optional) fee. (*Id.* ¶ 24.) Although a Tornado Cash smart contract known as the "Relayer Registry" could be used to identify a relayer, users did not have to select a relayer from this registry, and anyone could run a relayer node. Relayers could charge a fee by deducting a specified amount from the user's withdrawal, but this was not required. (*Id.*) Crucially, even with a relayer-assisted withdrawal, the user's tokens would be sent directly to the user; the relayers would never gain custody over the user's tokens. (Coin Center § 3.) Nor would the deposit note ever be shared with the relayer—the user would authorize a relayer-assisted withdrawal by interacting with the smart contract, not by sharing the deposit note with the relayer. (*Id.*) The use of a relayer was, at all times, optional, and the relayer determined whether to charge a fee and, if so, in what amount. (*Id.* ¶¶ 15, 24.)

5. Tornado Cash Community Governance and TORN Tokens

To further decentralize and ensure that no single entity or person could exert disproportionate influence over any Tornado Cash-related project, Peppersec, with input from the large Tornado Cash community, implemented a decentralized governance system that was put into effect on December 18, 2020. In connection with this effort, a decentralized autonomous organization ("DAO") was established to allow the community of users and developers of Tornado Cash to make collective decisions over the governance of the protocol.

(Ind. ¶ 26.) To facilitate the governance process, an Ethereum-based governance token called the TORN token was proposed. (*Id.* ¶ 27.)[8] In short, users and developers who sought to have an influence over future developments regarding Tornado Cash could create and/or vote on governance proposals by first acquiring and then depositing TORN into the Tornado Cash Governance smart contract. (*Id.* ¶ 28.) Participation in Tornado Cash governance is entirely optional; a user need not participate in governance to interact with the Tornado Cash pools, and a community member need not use the protocol in order to participate in the governance process. (Coin Center § 3.) Although relayers could acquire and stake TORN to be listed in the Relayer Registry (Ind. ¶ 30), as noted above, anyone could run a relayer node and act as a relayer in a Tornado Cash transaction,[9] whether or not that person was listed in the Relayer Registry. In no way and at no time did participation in the DAO, possession of TORN, or any other involvement in the governance mechanisms described here afford anyone any control over the immutable smart contracts or any funds users moved through those smart contracts in order to obtain the legitimate privacy benefits of Tornado Cash.

6. Tornado Cash Compliance Tool

In addition to a UI and website, Peppersec developed and made available a separate software application called the Tornado Cash Compliance Tool. It permitted users to generate a report that revealed, for a particular transaction, the source of the funds deposited into and later withdrawn from Tornado Cash. (Ind. ¶ 39.) Such cryptographically verified reports could be provided to any entity that required it—for example, in connection with a deposit to a

[8] *See* Tornado Cash, Tornado.cash compliance, Medium (Jun. 3, 2020), available at https://tornado-cash.medium.com/tornado-cash-compliance-9abbf254a370.

[9] The Indictment does not allege that Mr. Storm or the Peppersec developers themselves operated relayers.

cryptocurrency exchange that is subject to requirements under the Bank Secrecy Act, like Know Your Customer ("KYC") or Anti-Money Laundering ("AML") requirements. Like any UI, the Compliance Tool was optional; it did not affect the core operation of the Tornado Cash smart contracts. (*Id.*)[10] Indeed, because it was not coded at the protocol level when the smart contracts were deployed, it could not have been added when bad actors later allegedly used it for illicit purposes.

C. The OFAC Sanctions, Arrest of Alexey Pertsev, and Investigation and Indictment of Roman Storm

1. The OFAC Sanctions

On August 8, 2022, OFAC sanctioned Tornado Cash, naming it as a specially designated national ("SDN"), and added Tornado Cash along with numerous cryptocurrency wallet addresses associated with the Tornado Cash smart contracts to the SDN List under Executive Order 13694.[11] On November 8, 2022, OFAC simultaneously delisted and redesignated Tornado Cash as an SDN under Executive Orders 13694 and 13722,[12] and it provided further guidance on the sanctions. Neither the original OFAC sanction or its revision sanctioned any developer of Tornado Cash, TORN holders, or anyone associated with Tornado Cash DAO governance, including Mr. Storm.[13]

---

[10] *See* Tornado Cash, Tornado.cash compliance, Medium (Jun. 3, 2020), available at https://tornado-cash.medium.com/tornado-cash-compliance-9abbf254a370.

[11] Exec. Order No. 13694, 80 FR 18077, Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities.

[12] Exec. Order No. 13722, 81 FR 14943, Blocking Property of the Government of North Korea and the Workers' Party of Korea, and Prohibiting Certain Transactions With Respect to North Korea.

[13] Concurrently with the unsealing of the Indictment, OFAC sanctioned Roman Semenov, who is a foreign national. *See* https://home.treasury.gov/news/press-releases/jy1702.

The OFAC sanctions have been challenged in two federal court cases. The first was filed on September 8, 2022 in the Western District of Texas by six Ethereum users and is on appeal before the Fifth Circuit. *See Van Loon et al. v. Dep't of Treasury et al.*, Case No. 1:23-cv-00312 (W.D. Tex.). The second was filed on October 12, 2022 in the Northern District of Florida by Coin Center and three Ethereum users and is on appeal before the Eleventh Circuit. *See Coin Center et al. v. Yellen et al.*, Case No. 3:22-cv-20375 (N.D. Fla. Oct. 30, 2023).

2. The Arrest of Alexey Pertsev

Two days after OFAC's August 2022 sanctions announcement, on August 10, 2022, Mr. Pertsev was arrested in the Netherlands, where he was living and working.[14] Mr. Pertsev has been charged with money laundering. (*Id.*) In the Netherlands, unlike in the United States, a person can be guilty of money laundering based on personal negligence.[15] Mr. Pertsev's trial started on March 26, 2024, and is ongoing.

3. The Investigation and Indictment of Roman Storm

Soon after the OFAC sanctions were announced and Mr. Pertsev was arrested in August 2022, Mr. Storm learned that the government was investigating him. He was cooperative with the investigation, and he even met with law enforcement in this District on November 16, 2022, for a large part of the day to discuss Tornado Cash.

Despite his ongoing willingness to cooperate with law enforcement and explain why he had not violated any laws, on August 23, 2023, Mr. Storm was arrested at his home in the Seattle

[14] *See* Jack Schickler, *Tornado Cash Developer Alexey Pertsev to Remain in Jail Until at Least Late February*, CoinDesk (Nov. 23, 2022), available at https://www.coindesk.com/policy/2022/11/22/tornado-cash-developer-alexey-pertsev-to-remain-in-jail-until-at-least-late-februrary/.

[15] *See* European Union Anti Money Laundering Centre, Dutch Criminal Law, available at https://www.amlc.eu/dutch-criminal-law/ (explaining "culpable variation" of money laundering under Dutch Penal Code.)

area based on the pending Indictment. Mr. Storm, along with Mr. Semenov (who has not been arrested), is charged with three counts of conspiracy: (1) money laundering; (2) operating an unlicensed money transmitting business; and (3) violating the International Emergency Economic Powers Act ("IEEPA").

The Indictment contains numerous allegations that will be proven incorrect at trial if this motion is not granted. It also takes purported statements by Mr. Storm and others out of context and is silent on a number of important issues that undercut the government's theories of criminality. For example, the Indictment does not allege that Mr. Storm or the other Peppersec developers had any interactions with any hackers who allegedly misused the Tornado Cash protocol, including the Lazarus Group, which is alleged to be behind the Ronin hack. (*See* Ind. ¶¶ 56, 60.) The Indictment also does not allege that the Lazarus Group used the website or the Peppersec UI in connection with its alleged use of Tornado Cash. (*See id.* ¶¶ 58-68.)[16] And it does not allege what steps Mr. Storm or the Peppersec developers could have taken but refused to take to prevent the Lazarus Group from engaging directly with the by-that-time immutable Tornado Cash protocol (because there are none). Lastly, it does not allege that Mr. Storm was a relayer or that, after May 2020, he and the Peppersec developers had control over anything other than the website and the Peppersec UI.

III. LEGAL STANDARD ON MOTION TO DISMISS

"[An] indictment must contain an allegation of every fact which is legally essential [for] the punishment to be inflicted." *Apprendi v. New Jersey*, 530 U.S. 466, 512 (2000) (internal quotation marks omitted). As the Second Circuit has explained, "If [an] indictment does not

[16] The Indictment references a news article that described how a sanctions screen the Peppersec developers added to the Peppersec UI could have been evaded (*id.* ¶ 65), but this is not direct evidence that the Lazarus Group in fact used it.

state the essential elements of the crime, the defendant cannot be assured that he is being tried on the evidence presented to the grand jury." *United States v. Pirro*, 212 F.3d 86, 92 (2d Cir. 2000). Accordingly, a defect in an indictment, including a failure to state an offense, may be grounds for pre-trial dismissal. Fed. R. Crim. P. 12(b)(3)(B)(v). As the Second Circuit has instructed:

> Since federal crimes are "solely creatures of statute," *Dowling v. United States,* 473 U.S. 207, 213, 105 S. Ct. 3127, 87 L. Ed.2d 152 (1985), a federal indictment can be challenged on the ground that it fails to allege a crime within the terms of the applicable statute.

United States v. Aleynikov, 676 F.3d 71, 75–76 (2d Cir. 2012) (citing *Pirro,* 212 F.3d at 91-92). The district court must consider any indictment "as it was actually drawn, not as it might have been drawn." *See Pirro,* 212 F.3d. at 92 (citing *Sanabria v. United States,* 437 U.S. 54, 65–66 (1978) ("The precise manner in which an indictment is drawn cannot be ignored."")). A defendant who objects to the indictment before trial is entitled to an exacting review of it. *Id.* An indictment must be dismissed if "it fails to allege a crime within the terms of the applicable statute." *Aleynikov*, 676 F.3d at 75-76.

A further basis to dismiss an indictment is where undisputed evidence shows that the facts alleged do not constitute a crime. District courts may properly rule on a motion to dismiss an indictment when the undisputed evidence shows that, "as a matter of law, the [d]efendant could not have committed the offense for which he was indicted." *United States v. Todd*, 446 F.3d 1062, 1067-69 (10th Cir. 2006); *United States v. Weaver*, 659 F.3d 353, 355 n* (4th Cir. 2011) (dismissal appropriate where "the government does not dispute the ability of the court to reach the motion and proffers, stipulates, or otherwise does not dispute the pertinent facts"); *see also United States v. Quinones*, 313 F.3d 49, 59 (2d Cir. 2002) ("[W]e have previously considered purely legal challenges to criminal statutes raised during the pre-trial stage of a

prosecution even though the defendants had not yet been—and might never have been—convicted of violating the challenged statute.") (citing cases).

IV. ARGUMENT

For the reasons set forth below, the Indictment's three counts should be dismissed pursuant to Rule 12 for failure to state offenses. Each is fundamentally defective for certain distinct and, in certain cases, overlapping reasons. Because the grounds to dismiss Count One, conspiracy to commit money laundering, relies (in part) on analysis of the regulatory definitions discussed in connection with Count Two, conspiracy to operate an unlicensed money transmitting business, Count Two is addressed first. Next is a discussion of Count One and then Count Three. Following that, there is a discussion of why all the Counts should be dismissed on First Amendment and various Due Process grounds.

A. The Conspiracy to Operate an Unlicensed Money Transmitting Business Count (Count Two) Should Be Dismissed

Count Two should be dismissed because it fails to allege that Mr. Storm operated a "money transmitting business" as 18 U.S.C. § 1960 contemplates. The Indictment claims that Mr. Storm violated Section 1960 by: (1) failing to register what it refers to as the "Tornado Cash services" as a money service business (and meet the related requirements), in violation of Section 1960(b)((1)(B); and (2) knowing that this alleged money transmitting business was used to transfer criminal proceeds, in violation of Section (b)(1)(C). But none of the components of what the Indictment claims are the "Tornado Cash services"—taken separately or together—was a money transmitting business for at least two independent reasons: (1) users maintained exclusive control over their cryptocurrency; and (2) Tornado Cash did not charge a fee for transmitting funds. Thus, Count Two is fatally flawed and must be dismissed.

The Indictment asserts that the "Tornado Cash service" "provided a seamless and fully integrated service that executed anonymous transactions in ETH and certain other cryptocurrencies for its customers." (Ind. ¶ 10.) According to the Indictment, beyond the deployment of the Tornado Cash smart contracts themselves, its "principal operating features" included "a website and a user interface" and a "network of 'relayers' who provided customers with enhanced anonymity in exchange for a fee." (*Id.* ¶¶ 9-10.) The Indictment alleges that Mr. Storm conspired to violate Section 1960 by failing to register the "Tornado Cash service" with FinCEN as a money transmitting business, by failing to establish an effective AML program or engage in any KYC efforts, and because it facilitated the transfer of criminal proceeds. (*Id.* ¶¶ 33-35.) One overt act is included in the Indictment: Mr. Storm's purported use of Peppersec funds in May 2022 to pay for "web hosting services for the Tornado Cash website." (*Id.* ¶ 82.)

1. Statutory and Regulatory Provisions

Section 1960, which is part of the Bank Secrecy Act ("BSA"), starts out by stating in subsection (a):

> Whoever knowingly conducts, controls, manages, supervises, directs, or owns all or part of an ***unlicensed money transmitting business***, shall be fined in accordance with this title or imprisoned not more than 5 years, or both.

(Emphasis added.) And the statute goes on to explain in subsection (b):

> (1) the term "***unlicensed money transmitting business***" means a money transmitting business which affects interstate or foreign commerce in any manner or degree and—
>
> > (A) is operated without an appropriate money transmitting license in a State where such operation is punishable as a misdemeanor or a felony under State law, whether or not the defendant knew that the operation was required to be licensed or that the operation was so punishable;
> >
> > (B) fails to comply with the money transmitting business

> registration requirements under section 5330 of title 31, United States Code, or regulations prescribed under such section; or
>
> (C) otherwise involves the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity;
>
> (2) the term "***money transmitting***" includes transferring funds on behalf of the public by any and all means including but not limited to transfers within this country or to locations abroad by wire, check, draft, facsimile, or courier[.]

(Emphasis added.)

Section 1960's definition of a "money transmitting business" has been interpreted to be coextensive with the BSA's definition of that same phrase. *See* 31 U.S.C. § 5530(d)(1); *see also, e.g., United States v. Budovsky,* 2015 WL 5602853, at *8 (S.D.N.Y. Sept. 23, 2015). Section 5330 is a provision of the BSA that requires the owner of a "money transmitting business" to register with the Secretary of the Treasury. 31 U.S.C. § 5330(a)(1). The definition of a "money transmitting business" in Section 5330 includes both (i) a "money transmitting service," which includes persons "***accepting*** currency, funds, or value that substitutes for currency and ***transmitting*** the currency, funds, or value that substitutes for currency by any means"; and (ii) "any other person who engages as a business in the transmission of currency, funds, or value that substitutes for currency." 31 U.S.C. §§ 5330(d)(2), (d)(1)(A) (emphasis added).

While Section 5330 broadly defines money transmitting business, the BSA requires and empowers the Secretary of Treasury to further define which businesses are obligated to register and what their compliance obligations should be. *See California Bankers Association v. Shultz*, 416 U.S. 21, 64 (1974) ("the statute is not self-executing, and were the Secretary to take no action whatever under his authority, there would be no possibility of criminal or civil sanctions

being imposed on anyone"). Therefore, it is the regulatory definition of money transmitter, promulgated by the Secretary, that bears the most relevance in this case.

The implementing regulations for Section 5330 are administered by the U.S. Treasury Department's Financial Crimes Enforcement Network ("FinCEN") in 31 C.F.R. § 1010.100 *et seq.* (together, the "FinCEN Regulations"). The FinCEN Regulations require that "each money services business . . . must register with FinCEN" except if it falls within certain enumerated exceptions. 31 C.F.R. § 1022.380(a)(1). A "money services business" ("MSB") is defined as "[a] person wherever located doing business, whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part within the United States, in one or more of the capacities" enumerated in the FinCEN Regulations. 31 C.F.R. § 1010.100(ff). One such category of MSB is a "money transmitter," which is either (i) someone who provides "money transmission services," defined as "the ***acceptance*** of currency, funds, or other value that substitutes for currency from one person *and* the ***transmission*** of currency, funds, or other value that substitutes for currency to another location or person by any means"; or (ii) "[a]ny other person engaged in the ***transfer*** of funds." *Id.* § 1010.100(ff)(5)(i) (emphasis added). Specifically, exempted from the definition of "money transmitter" are individuals who merely provide "the delivery, communication, or network access services used by a money transmitter to support money transmission services." *Id.* § 1010.100(ff)(5)(ii)(A).

2. The Indictment Fails to Allege that Roman Storm or Tornado Cash Had the Requisite Control to Be a Money Transmitting Business

The Indictment's allegations are insufficient to state an offense because control of the funds (in this case, cryptocurrency) being transmitted is a prerequisite to being a money transmitter, and no alleged component of the "Tornado Cash service" ever had such control. Control is a prerequisite because the language "acceptance" and "transmission", by its very

nature, requires the entity or individual who is the "money transmitting business" to take control of the funds otherwise they cannot and are not actually accepting them and transmitting or transferring them. Second Circuit interpretations of Section 1960 adopt an approach that requires possession and control of the funds being transmitted. *See United States v. Velastegui*, 199 F.3d 590, 592 (2d Cir. 1999) (money transmitting business "***receives*** money from a customer and then, for a fee paid by the customer, ***transmits*** that money to a recipient") (emphases added); *see also United States v. Bah*, 574 F.3d 106, 114 n.6 (2d Cir. 2009) (violation of Section 1960 occurs when an individual "maintain[s] possession" of and then "transfer[s]" someone else's funds).

Dictionary definitions are in accord. "[T]ransmit" means "to send or transfer (a thing) from one person or place to another."[17] "Transfer" similarly means "to convey from one person, place, or situation to another," or "to cause to pass from one to another."[18] One cannot convey something from one person or place to another without having control over that thing. And in legal parlance, "transfer" refers to "[a]ny mode of disposing of or parting with an asset or an interest in an asset."[19] One cannot dispose of an asset or an interest in an asset unless one has control over the asset. Likewise, to "accept" something means "to receive (something offered) willingly."[20] "Receive," in turn, has been interpreted to mean "to acquire control, in the sense of

[17] *Transmit*, Black's Law Dictionary (11th Ed. 2019); *see also* Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/transmit ("to send or convey from one person or place to another").

[18] *Transfer*, Merriam-Webster Dictionary Online, available at https://www.merriam-webster.com/dictionary/transfer.

[19] *Transfer*, Black's Law Dictionary (11th Ed. 2019).

[20] *Accept*, Merriam-Webster Dictionary Online, available at https://www.merriam-webster.com/dictionary/accept.

physical dominion or apparent legal power to dispose of the [item]."[21] *United States v. Stanley*, 896 F.2d 450, 451 (10th Cir. 1990); *see also United States v. Dobbs*, 629 F.3d 1199, 1203-04 (10th Cir. 2011) ("to receive" means "to accept an object and to have the ability to control it"). The exemption for providing network access services emphasizes the point that it is not enough to provide a service that supports the money transmission of others, but rather, the party must have sufficient control over the funds to effect a transfer or transmission of the funds.

Guidance from FinCEN itself reinforces this point when it discusses how, for example, a cryptocurrency wallet provider must have "total independent control" over what is being transmitted to be a money transmitter. (FinCen Guidance, FIN-2019-G001, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (May 9, 2019), at 15.) FinCEN's guidance explains that intermediaries such as "multiple-signature wallet providers" are not "money transmitter[s]" because, even though they are necessary to effectuate a transaction, the intermediary "does not have total independent control over the value." (*Id.* at 17.) Thus, although not binding, FinCEN itself recognizes that control is a touchstone of what makes a party a money transmitting business. (Int'l Academy at 7-8.)

The Indictment does not allege Mr. Storm or the Peppersec developers had independent control over Tornado Cash user funds. Nor could it, because the "secret note"—which permits the user to access and use the funds—is only in the possession of the user and is not shared with anyone (unless they choose to share it). (Coin Center § 3; Int'l Academy at 12-13.) The Indictment's allegations regarding Mr. Storm's control over the Peppersec UI are insufficient because it did not access the funds directly; it merely provided an interface to permit a user's

[21] *Receive,* Merriam-Webster Dictionary Online, available at https://www.merriam-webster.com/dictionary/receive.

wallet to interact with the smart contracts. As the Indictment explains, when using the Tornado Cash smart contracts through the UI, a user "could connect [their] Ethereum wallet to the UI, and . . . could then simply go to the "Deposit" tab, select the amount of ETH to be deposited from one of four choices . . . and then connect to execute the transaction." (Ind. ¶ 15.) In plain language, the Indictment explains that it is the user who initiates the transaction. The same goes for withdrawals: "To make a withdrawal from the Tornado Cash service, the [user] would go to the "Withdraw" tab on the UI and enter the secret note that the customer had received when making the deposit, along with the recipient address where the withdrawal should be transmitted." (*Id.* ¶ 16.) The Peppersec UI did not store the secret note. (Int'l Academy at 11.) Put simply, any cryptocurrency a user intended to send to a Tornado Cash pool went from the user to the pool (and back) and were never in the custody or control of the Peppersec UI or Mr. Storm himself.

The relayers also lacked any direct contact with a user's assets. Rather, even with a relayer-assisted withdrawal, the user's tokens would be sent directly to the user; the relayers never gain custody or control over the user's tokens. (Coin Center§ 3.) Further, a relayer who failed to relay the requested transaction message does not get to keep any associated tokens and has no effect on the user's control of their tokens; the user could simply send the same message via a different relayer or choose not to use a relayer at all and the user would still receive their withdrawal. (Coin Center § 3; Int'l Academy at 15.)

Nor did Mr. Storm and the Peppersec developers have any control over the smart contracts themselves. Even under the false assumption that allegations regarding their control over the development of the Tornado Cash smart contracts would be sufficient, Mr. Storm and the Peppersec developers relinquished any control they had by May 2020, when Tornado Cash

became immutable (*see* Ind. ¶ 26), which is before the operative timeframe of the alleged money transmitting conspiracy. (*Id.*. ¶ 77.) Accordingly, the Tornado Cash "services", even as alleged and in the light most favorable to the government, do not meet the definition of a money transmitter and instead fall under the "network access services" exemption.

3. The Indictment Fails to Allege that Roman Storm or Tornado Cash Charged a Fee for the Transfer of Funds

Count Two of the Indictment also fails because it does not allege that Mr. Storm and the Peppersec developers or Tornado Cash charged any fee for transmitting funds. The Second Circuit, in interpreting Section 1960, has made clear that a money transmitting business is one that charges a fee for the service of transmitting funds. As the Second Circuit stated in *Velastegui*: "A money transmitting business receives money from a customer and then, ***for a fee paid by the customer***, transmits that money to a recipient in a place that the customer designates, usually a foreign country." 199 F.3d at 592 (emphasis added); *see also United States v. Banki,* 685 F.3d 99, 113 n.9 ("the business must transmit money to a recipient in a place that the customer designates, ***for a fee paid by the customer***") (emphasis added). Tornado Cash was then not a money service business for the additional reason that it did not charge a user any fee to use it.

Mr. Storm and the Peppersec developers also did not charge a fee to transmit money on behalf of users. The Indictment alleges that they independently profited for their Tornado Cash development efforts through their receipt and sale of TORN tokens, which permitted holders to make governance decisions involving the DAO (which itself had certain governance control over future or additional projects concerning Tornado Cash). (Ind. ¶¶ 26-28, 69-75.) But nowhere does the Indictment allege that any fee was charged or earned for any transmission of cryptocurrency using Tornado Cash other than by the relayers. Further, the Indictment does not

allege that Mr. Storm ran a relayer; relayer operators were third parties who operated independently (and they did not receive, transmit, or touch any funds). Because neither Mr. Storm nor Tornado Cash charged a fee, Count Two fails for this additional reason.

B. The Conspiracy to Commit Money Laundering Charge (Count One) Should Be Dismissed

The Indictment's money laundering conspiracy charge has numerous defects that require dismissal. As an initial matter, as charged in the Indictment, a conspiracy to commit money laundering requires someone to engage in a "financial transaction" involving a "financial institution," but there are no "financial transactions" that come within the reach of the statute because, as discussed above, what the government calls the "Tornado Cash service" is not a money transmitting business under 18 U.S.C. § 1960.

Even if the Indictment had alleged a "financial transaction" involving a "financial institution," its money laundering conspiracy charge would nevertheless fail because it does not allege either that Mr. Storm entered into an unlawful agreement with any person who used Tornado Cash smart contracts or the Peppersec UI for illicit purposes, or that he had the specific intent to commit money laundering. The Indictment also fails to allege the necessary criminal *mens rea*. As such, the Indictment fails to state an offense and Count One should be dismissed.

1. The Alleged "Financial Transaction(s)" Do Not Come Within Section 1956 Because Tornado Cash Was Not a "Financial Institution"

The Indictment alleges that Mr. Storm conspired to conduct an illicit "financial transaction" involving the use of a "financial institution." (Ind. ¶ 78.) This theory fails for the same reasons as Count Two—Tornado Cash is not a money transmitting business.

Section 1956 defines a "financial transaction" as, among other things, "a transaction involving the use of a financial institution which is engaged in, or the activities of which affect, interstate or foreign commerce in any way or degree." 18 U.S.C. § 1956(c)(4)(B). A "financial

institution," under Section 1956(c)(6)(A), then looks to the BSA definition of a "financial institution" under 31 U.S.C. § 5312(a)(2), and its implementing regulations. In turn, Section 5312(a)(2) references various types of financial institutions, such as banks and brokerages and persons engaged as a business in money transmission; the only type applicable to the Indictment is money transmission. 31 U.S.C. § 5312(a)(2)(R) ("person who engages as a business in the transmission of currency, funds, or value that substitutes for currency," including "any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system"); *see also* 31 U.S.C. § 5330 (d)(1) (applying same definition to "money transmitting business"). *See, e.g., United States v. Ness*, 565 F.3d 73, 79 (2d Cir. 2009) (analyzing "Section 5312(a)(2) and the regulations promulgated thereunder" for definition of "financial institution" under Section 1956(c)(6)) and rejecting government's theory that defendant acted as a money transmitter "and was, therefore, a financial institution").

Accordingly, Count One must be dismissed on the same basis that Count Two must be dismissed. For the reasons discussed in Section IV(A) above, which are incorporated herein by reference, no component of the alleged "Tornado Cash service"—together or separately—was a money transmitting business. First, no component of the alleged Tornado Cash service ever had control over the cryptocurrency transmitted, because Tornado Cash was programmed to provide users full control over their funds. Second, the Tornado Cash protocol—the only component of the alleged service to touch any cryptocurrency—did not charge any fee but was a free and open-source software tool. *See Banki*, 685 F.3d at 113 ("business" must function as an "enterprise" "conducted for a fee or profit"); *Velastegui*, 199 F.3d at 592, 595 n. 4 (2d Cir.1999) ("money

transmitting business" is the transmission of money "for a fee"). Thus, Count One is defective and should be dismissed.

2. Roman Storm Did Not Conspire or Agree with Anyone to Conduct a Financial Transaction Involving the Proceeds of Specified Unlawful Activity

Even if any component of the alleged Tornado Cash "service" were a money transmitting business, Count One fails because it lacks any allegations to support a criminal conspiracy involving Mr. Storm.

The charged object of the purported conspiracy is concealment money laundering in violation of 18 U.S.C. § 1956(a)(1)(B)(ii). Conspiracy, "'is the agreement . . . to commit one or more unlawful acts.'" *United States v. Jones*, 482 F. 3d 60, 72 (2d Cir. 2006) (quoting *Braverman v. United States*, 317 U.S. 49, 53 (1942)). To convict Mr. Storm of Count One, the government must prove that he agreed with someone else to violate the federal money laundering statute, and "knowingly engaged in the conspiracy with the specific intent to commit the offenses that [are] the objects of the conspiracy." *United States v. Garcia*, 587 F.3d 509, 515 (2d Cir. 2009); *see also United States v. Threadgill*, 172 F.3d 357, 366 (5th Cir. 1999) (defendant must "join[] the agreement knowing its purpose and with the intent to further the illegal purpose").

(a) <u>The Indictment fails to allege facts showing an agreement between Mr. Storm and any criminal hackers</u>.

The Indictment does not allege facts that could even come close to meeting this standard, because it alleges no contact of any kind between the alleged bad actors and Mr. Storm and the Peppersec developers.

There is nothing unlawful about the alleged agreement between Mr. Storm and the Peppersec developers to "develop[] the Tornado Cash [protocol]," when they publicly launched the protocol in August 2019. (*See* Ind. ¶ 9.) The Indictment does not allege it was unlawful to

develop and release the Tornado Cash smart contracts directly to users and the public, or that it was unlawful to make an open-source UI available to interact with the Tornado Cash smart contracts, or that it was unlawful to develop a website so that users could have information about and access to the Tornado Cash smart contracts "using any standard internet browser." (*See id.* ¶ 14.) Thus, the Indictment's own allegations make clear that the only agreement Mr. Storm participated in was a lawful one to develop open-source software to permit users "to send Ethereum cryptocurrency 100% anonymously using groundbreaking, non-custodial technology based on strong cryptography[.]" (*See id.* ¶ 9.)

This is a problem for the government, because Tornado Cash was immutable in May 2020, four months before the alleged start to the "conspiracy." (*See id.* ¶¶ 26, 77). Neither Mr. Storm nor the other developers had any further ability to change how the smart contracts operated or prevent anyone with an internet connection from accessing and using them. The only "agreement" at this time was the lawful agreement to publish open-source code to permit financial privacy on the Ethereum blockchain.

The Indictment's failure to allege any relationship between Mr. Storm and the alleged third-party bad actors is fatal to the alleged money laundering conspiracy because it fails to allege a basic element—either an explicit agreement or an implicit agreement manifested through mutual interdependence of the alleged co-conspirators. *See United States v. Maldonado-Rivera*, 922 F.2d 934, 963 (2d Cir. 1990) (requiring "sufficient proof of mutual dependence and assistance"); *see, e.g., United States v. Figueroa*, No. 08 CR 749 (ARR), 2010 WL 11463852, at *10-11 (E.D.N.Y. Mar. 2, 2010) (defendant granted acquittal of conspiracy to distribute charge because the evidence "d[id] not raise even a suggestion . . . that those transactions and the participants in those transactions were mutually dependent upon, interrelated with, or had a

shared common goal with either each other or the [charged] conspiracy"); *see also United States v. Chandler*, 388 F.3d 796, 811 (11th Cir. 2004) ("the government must show an interdependence among the alleged co-conspirators."); *United States v. Abdelaziz*, 68 F.4th 1, 49 (1st Cir. 2023) ("Without interdependence . . . the tacit understanding necessary for these defendants to have agreed to conspire . . . does not exist.") (internal quotations and citation omitted); *United States v. Swafford*, 512 F.3d 833, 842 (6th Cir. 2008) (a single conspiracy did not exist due to lack of proof of actions "in furtherance of a common goal" or "significant interdependence among" the alleged conspirators). But here there is no such relationship.

To the contrary, the Indictment's allegations confirm that Mr. Storm and the Peppersec developers did not engage with, or have any contact with, any alleged bad actors; nor did they combine their efforts together toward a common (unlawful) goal. There is simply no allegation that the alleged bad actors—having an internet connection and access to open-source software—needed anything more from the developers; conversely, the developers had no dependence on the alleged bad actors.

Since there is no allegation of any agreement between Mr. Storm and any alleged bad actors (because it never happened), the government resorts to making one up by intentionally conflating the agreement to develop and publish Tornado Cash code with a (non-existent) agreement to engage in purported concealment money laundering, based on nothing more than the allegation that some (unidentified) third-party bad actors used the "Tornado Cash service"[22] for illicit purposes. The Indictment is utterly devoid of any supporting facts, relying instead on a *non sequitur* that (i) Mr. Storm and others developed Tornado Cash and (ii) it was (allegedly)

[22] By glomming together the Tornado Cash smart contracts with the UI and the relayer network under one misleading label, the government avoids clarifying whether any of the alleged hacks used the Peppersec UI at all, or merely accessed the (immutable) smart contracts.

misused by some criminals, and therefore (iii) the developers and alleged criminals must have conspired. Tellingly, there is no explanation of how the developers and the alleged criminals came to any agreement, nor is there any other allegation that Mr. Storm had a meeting of the minds with the alleged bad actors. (*See id.* at ¶¶ 47-49, 56-61.)

(b) The Indictment improperly seeks to convict Roman Storm based on a negligence theory of criminal money laundering.

Recognizing that in fact Mr. Storm and the other two co-developers had no interaction with any bad actor and did not move, hide, or even touch any criminal proceeds, the government ultimately makes clear that what it is urging is a negligence standard for criminal money laundering liability. That is, the Indictment claims that because Mr. Storm and the others did not implement KYC/AML into the UI, they should bear criminal responsibility for the actions of other third parties who used the Tornado Cash smart contracts. (*See, e.g.*, Ind. ¶ 42 ("Tornado Cash founders had the ability to implement . . . compliance features into the Tornado Cash UI"); *id.* ¶ 50 ("[T]he Tornado Cash founders *took no steps* to implement effective AML or KYC programs."); *id.* ¶ 66 (after Ronin hack, defendants "*took no action to prevent* the Tornado Cash [protocol] from facilitating this money laundering and sanctions evasions") (emphasis added).)

This would be a breathtakingly dangerous expansion of criminal liability, which is problematic *per se* and also as applied to this case. The government tacitly concedes that the alleged crimes—involving computer intrusion and wire fraud—were conducted by third parties with whom Mr. Storm had no contact whatsoever. This is clear from the Indictment's repeated use of the passive voice to describe the criminal acts of these third parties, some of which are not identified: (1) in September 2020, "a cryptocurrency exchange . . . suffered a hacking incident," and proceeds from the hack "were deposited into the Tornado Cash [protocol]" (Ind. ¶ 47); (2) in December 2021, a "cryptocurrency exchange . . . suffered a security breach caused by a stolen

private key," and proceeds from the hack "were deposited into the Tornado Cash [protocol]" (*id.* ¶ 48); (3) shortly after the March 29, 2022 Ronin Network hack, "hackers began depositing the proceeds of the hack into the Tornado Cash [protocol]" (*id.* ¶ 58). Although the Indictment alleges that Mr. Storm and the Peppersec developers learned about the illicit acts, at no point does it allege that they had a meeting of the minds with these alleged bad actors to help them launder the proceeds of their crimes (*see id.* at ¶¶ 47-49, 56-61), and they did not. But the government cannot find the bad actors, so it seeks to scapegoat Mr. Storm for lawfully developing open-source code for use by law-abiding citizens.

The government tries to mask the dangerous and glaring legal deficiency in its charging theory with scare tactics. It portrays Tornado Cash as a tool for North Korea (Lazarus Group) and the other unidentified criminal hackers to fund illicit activities through separate criminal money laundering conspiracies. But the alleged examples all occurred *after* May 2020, when Tornado Cash was already publicly available to anyone with an internet connection and "no one could further modify [the Tornado Cash] smart contracts." (*See id.* ¶ 26.) There is no allegation that Mr. Storm and the Peppersec developers had any contact with any North Koreans or any criminal hackers, that he had any control over their alleged misuse of Tornado Cash, or that he had any control over the proceeds of hacks allegedly deposited into Tornado Cash. The alleged money laundering conspiracy did not begin until well after the Tornado Cash smart contracts became public and immutable (*see id.* ¶ 77), and Mr. Storm and the Peppersec developers are not alleged to have touched the alleged criminal proceeds in any way.

Moreover, the Indictment concedes this was impossible because, post-immutability, Peppersec did not control the Tornado Cash protocol, which was designed to permit users to interact anonymously with it. (*Id.* ¶ 13.) It does not matter that the protocol was accessible

through the Peppersec UI because the UI did not give Mr. Storm (or Peppersec) access to, or control over, the crypto assets of UI users; as explained in the Indictment, users initiate and conduct their own transactions and the UI merely generates the transaction requests that are sent from the users' wallets to the smart contracts. (*See id.* ¶¶ 15-16.) Alternatively, of course, users could "send[] funds to the Tornado Cash pools by interacting with the smart contracts directly, thereby bypassing the UI." (*Id.* ¶ 13.) Different means, but same result—the users were interacting with the smart contracts, not with Mr. Storm or Peppersec.[23]

Finally, the government cherry-picks messages between Mr. Storm and the Peppersec developers, but even the government's curated version of events fails to establish conspiratorial intent. "[G]uys we are fucked" is the reaction one would expect from someone experiencing a cyberattack from a criminal hacking group. (*Id.* ¶ 61.) It is also normal to want to offer reassurance to the public regarding legal compliance (*id.* ¶ 63 ("[W]e need to tell everyone urgently that we do not let such individuals on the front")), and to express concerns about consequences for sanctions violations. (*id.* ("a guy got 5 years of incarceration for sanctions"), *id.* ¶ 64 ("law enforcement is reading them too and can use them against us later"). These expressions of apprehension, and fear of legal exposure are not surprising, and fail as a matter of law to show a meeting of the minds with the alleged bad actors.

The government's misguided attempt to proceed on a negligence theory should be rejected. A failure to prevent a bad act is not the same as an agreement to assist it. To prove conspiracy, "the government must show that two or more persons entered into a joint enterprise

[23] Given that this was a user-driven function, it makes perfect sense that Peppersec then offered users—the persons interacting with Tornado Cash, through whatever means they selected—a compliance tool permitting them to "document their own transaction history" (Ind. ¶ 39) to verify their sources of funds to regulated financial institutions or exchanges.

for an unlawful purpose, with awareness of its general nature and extent." *United States v. Khalupsky*, 5 F.4th 279, 288 (2d Cir. 2021). It must "show that each alleged member agreed to participate in what he knew to be a collective venture directed toward a common goal." There is no such evidence here. Accordingly, because there is "not a whit of evidence" that Mr. Storm "shared a common goal" with the alleged bad actors, the "conspiracy charged in the indictment "[is], in substance, a product of the [g]overnment's imagination." *See United States v. Johansen*, 56 F.3d 347, 351 (2d Cir. 1995).

3. Roman Storm Did Not Have the Specific Intent to Further an Illegal Purpose

The Indictment also fails to allege that Mr. Storm had a criminal *mens rea*, and he did not. There are simply no allegations that he "knowingly engaged in the conspiracy with the ***specific intent*** to commit the offenses that [are] the objects of the conspiracy." *Garcia*, 587 F.3d 509, 515 (emphasis added).

There is not one single allegation in the Indictment, as fairly read, that would establish that Mr. Storm knew that a conspiracy existed to conduct financial transactions to conceal the proceeds of criminal activities and joined that conspiracy specifically intending to commit those offenses. The Indictment seeks to conflate an intent to design and promote a protocol for financial privacy in the Indictment with a specific intent to conduct transactions involving illicit proceeds for the purpose of concealing those proceeds, but they are not the same. For example, the Indictment alleges that Mr. Storm and his two co-developers intended to design a software protocol that could allow users to "conduct anonymous and virtually untraceable financial transactions." (Ind. ¶ 10.) This represents only the intent to permit Ethereum users to have financial privacy when conducting their own blockchain transactions, and is a far cry from the specific intent required to enter a money laundering conspiracy.

Indeed, the fact that the developers' intent to build the protocol happened first, and the criminal activity came afterward, undermines any inference of specific intent. The Tornado Cash smart contracts were immutable in May 2020, but each alleged computer intrusion or fraud incident happened after that, and the alleged conspiracy is not even alleged to have begun until September 2020. (*See, e.g.,id.* ¶¶ 26, 46-48, 56, 77.) The Indictment's own chronology thereby undermines any possible showing of specific intent on the part of Mr. Storm and the developers to join a money laundering conspiracy, because there were no criminal proceeds at issue until the protocol was already deployed and unchangeable. *See United States v. Fallon*, 61 F.4th 95, 120 (3d Cir. 2023) ("[A] money-laundering transaction can only occur *after* funds obtained from unlawful activity (*e.g.*, fraud schemes) are delivered into the defendant's possession.") (emphasis in original); *United States v. Conley*, 37 F.3d 970, 980 (3d Cir. 1994) ("proceeds" for the money laundering statute "are derived from an already completed offense, or a completed phase of an ongoing offense, before they can be laundered").

Further, as discussed above (*see* Section IV.B.3 *supra*), the government's case ultimately rests on the proposition that, because the developers learned along the way that alleged bad actors were using the Tornado Cash smart contracts to launder the proceeds of illegal activities, they should have avoided promoting Tornado Cash, or taken steps to prevent bad actors from using the smart contracts. But just as these negligence-based allegations fail to show a meeting of the minds with bad actors, they also undermine any claim that there was any specific intent to conspire with the bad actors to conceal the illicit proceeds of their crimes. A failure to take affirmative steps to try to block someone from engaging in bad conduct does not establish an intent to further or assist in that conduct. "A defendant's "mere presence at the scene of a criminal act or association with conspirators does not constitute intentional participation in the

conspiracy, even if the defendant has knowledge of the conspiracy." *United States v. Lorenzo*, 534 F.3d 153, 159-60 (2d Cir. 2008) (reversing conspiracy conviction where defendant "was present at and participated in events that furthered the conspiracy," but "there [was] insufficient evidence to show that he did so knowingly and with the specific intent to further . . . the conspiracy"). Likewise, the presence of the Tornado Cash smart contracts in the public domain, the building of software tools like the UI to access them, and the promotion of Tornado Cash for lawful means are all insufficient to support an inference that Mr. Storm intentionally participated in the conduct of purported bad actors.

Finally, the Indictment's allegations regarding the promotion and potential profits from the protocol also fail to satisfy the specific intent element. (*See* Ind. ¶¶ 27-31, 69-75.) The Indictment suggests that, after allegedly learning that some bad actors were using the Tornado Cash smart contracts to conceal the proceeds of their crime, it was somehow nefarious that Mr. Storm and the others continued to promote the Tornado Cash protocol and hoped ultimately to profit (indirectly) from its adoption through potential increased demand for TORN, the DAO's governance token. (*See id.* ¶¶ 71-72.) The motive for profit is not unusual and does not support a specific intent to conspire to conduct unlawful activity. There are myriad examples of situations in which criminals have seized upon lawful tools for unlawful ends, regardless of the intent of the tools' developers, and the tools' developers have profited from that use. *See, e.g., Twitter, Inc. v. Taamneh*, 598 U.S. 471, 449-501 (2023) (holding that Twitter, Google, and Facebook were not liable to terrorist attack victims, even though ISIS and its supporters used the social media sites to recruit, fundraise, and spread messages because the social media companies had no duty to stop the users and "[t]he mere creation of those platforms.. is not culpable… [even though] bad actors like ISIS are able to use platforms like defendants' for illegal—and

sometimes terrible—ends."); *Risley v. Universal Navigation Inc.,* 22 Civ 2780 (KPF), 2023 WL 5609200, at *14 (S.D.N.Y. Aug. 29, 2023) ([t]his [case] is less like a manufacturing defect, and more like a suit attempting to hold an application like Venmo or Zelle liable for a drug deal that used the platform to facilitate a fund transfer. There, as here, collateral, third-party human intervention causes the harm, not the underlying platform."). That does not mean the developers and purported criminals are in a conspiracy, and it certainly does not show a specific intent on the part of the Tornado Cash developers to engage in the concealment of illicit proceeds, which is required to convict them of a conspiracy to engage in money laundering.

C. The Conspiracy to Violate the IEEPA (Count Three) Should Be Dismissed Pursuant to the Statutory "Informational Materials Exception" and Because the Government Fails to Allege that Roman Storm Willfully Conspired to Evade Sanctions on North Korea

1. The IEEPA's "Informational Materials" Exception Requires Dismissal

The IEEPA conspiracy charge (Count Three) is based on the allegation that Mr. Storm conspired with others to develop and operate the "Tornado Cash service" for the purpose of evading North Korean sanctions. (Ind. ¶¶ 1, 84-88.) As explained above, that "service" allegedly consists of smart contracts and the UI (available through a website), both of which are available on the Internet to users of the Ethereum blockchain and are integral to the alleged conspiracy. (*Id.* ¶¶ 9, 10, 35.) As explained below, because the IEEPA's "informational materials" exemption applies to all alleged components of Tornado Cash, the government may not impose criminal liability on Mr. Storm.

(a) Informational materials, including software, are protected and exempted from the IEEPA prohibitions.

The President lacks the authority under the IEEPA to regulate information and informational materials:

> The authority granted to the President by this section does not include the authority to regulate or prohibit, ***directly or indirectly***
> ....
> (3) the importation from any country, or the exportation to any country, ***whether commercial or otherwise***, ***regardless of format or medium of transmission***, of any information or informational materials, including but not limited to, publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD–ROMs, artworks, and news wire feeds.

50 U.S.C. § 1702(b)(3) (emphasis added); *see also* 31 C.F.R. § 510.213(c).

The informational materials exemption was enacted in 1988, in what is known as the "Berman Amendment." *See Cap. Cities/ABC, Inc. v. Brady*, 740 F. Supp. 1007, 1009 (S.D.N.Y. 1990). "The Berman Amendment was designed to prevent the executive branch from restricting the international flow of materials protected by the First Amendment." *Kalantari v. NITV, Inc.*, 352 F.3d 1202, 1204-05 (9th Cir. 2003). In 1994, Congress "expanded the exemption's nonexclusive list of informational materials to include new media, such as compact discs and CD ROMs, and it clarified that the exemption applied to importation and exportation in any '***format or medium of transmission***.'" *Id.* at 1205 (emphasis added). Congress was concerned that "the Treasury Department has narrowly and restrictively interpreted the language in ways not originally intended," so it expanded the list of protected materials and prohibited both direct and indirect regulations thereof. H.R. Conf. Rep. No. 103–482, at 239, 1994 WL 151669 (1994), *reprinted in* 1994 U.S.C.C.A.N. 398, 483 (stating the intent to "facilitate transactions and activities incident to the flow of information and informational materials").

Courts in this Circuit have not had the occasion to apply the informational materials exemption to software,[24] but it is well established that software is speech subject to First

[24] This Court previously found an argument applying the informational materials exemption to software to be unripe. *See Open Soc'y Just. Initiative v. Trump*, 510 F. Supp. 3d 198, 213–14 (S.D.N.Y. 2021). In 1997, a California court held that the exemption did not apply to encryption software, but this was because the encryption software in that case was controlled for

Amendment protections. *See Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 449–50 (2d Cir. 2001) ("computer code conveying information is 'speech' within the meaning of the First Amendment"); *Bernstein,* 974 F. Supp. at 1308 (encryption software regulations unconstitutional prior restraint in violation of First Amendment). Thus, applying the informational materials exemption to the Tornado Cash software aligns with the goals of the exemption. *See Kalantari,* 352 F.3d at 1205; *Cernuda v. Heavey*, 720 F. Supp. 1544, 1553 (S.D. Fla. 1989) (discussing First Amendment concerns motivating informational materials exemption).

(b) The IEEPA charge impermissibly seeks to penalize Roman Storm for making informational materials (Tornado Cash software) available on the Internet.

The IEEPA conspiracy charge impermissibly seeks criminal sanctions against Mr. Storm for his role in publishing one piece of software (Tornado Cash) on top of another (Ethereum blockchain). Tornado Cash is software. It uses smart contracts. (Ind. ¶ 10 ("smart contracts hosted on the Ethereum blockchain"), ¶ 11 ("It uses a smart contract"), ¶ 13 ("sending funds to the Tornado Cash pools by interacting with the smart contracts directly"). Smart contracts are computer code. (*Id.* ¶ 8 ("the smart contract's code"), ¶ 35 (describing "computer code relating to the Tornado Cash service").) Tornado Cash is published on the Ethereum blockchain (*id.* ¶¶ 10, 17), which is also computer code operating on a public network of computers. (*Id.* ¶ 4 (ETH "is generated and controlled automatically through computer software operating on a 'peer to peer' network"), ¶ 7 (network is "the Ethereum peer-to-peer network").) These are informational materials shielded from IEEPA regulation. The indictment itself complains that Mr. Storm

export under the Export Administration Act, and Congress expressly carved export-controlled items out of the Berman Amendment. *Bernstein v. U.S. Dept. of State*, 974 F. Supp. 1288, 1303 (N.D. Cal. 1997); 50 U.S.C. § 1702(b)(3). There is no allegation that the Tornado Cash software was controlled for export (it was not).

allegedly published "documents with ***information*** and guidance on how to use the Tornado Cash service." (*Id.* ¶ 35 (emphasis added).)

The charged transactions are those of Lazarus Group (not Mr. Storm) as part of its alleged ongoing misuse of the Tornado Cash smart contracts to deposit cryptocurrency (ETH) from the Ronin hack. (*Id.*. ¶¶ 58, 66, 68.) In other words, the charge of sanctions evasion is based on Lazarus Group's alleged misuse of the Tornado Cash software that Mr. Storm and others published on the Internet.

The government cannot avoid the informational materials exemption by calling Tornado Cash software a "service." (*See*, *e.g.*, *id.* ¶ 1 ("a cryptocurrency mixing service known as Tornado Cash"). The IEEPA regulations may not extend to a "service" if doing so constitutes indirect regulation of informational materials. 50 U.S.C. § 1702(b)(3) (the President has no "authority to regulate or prohibit, ***directly or indirectly***" (emphasis added)); *see also Marland v. Trump*, 498 F. Supp. 3d 624 at 638 (E.D. Pa. 2020) (explaining that the exemption "extend[s] even to regulations that do not on their face regulate the exchange of informational materials, but nevertheless have such an effect"). This is why the government was prohibited from shutting down TikTok even though it allegedly could be used by China to spy on Americans. The government's "prohibitions 'indirectly' 'regulate' the transmission of 'informational materials' by U.S. persons." *TikTok Inc. v. Trump*, 490 F. Supp. 3d 73, 81 (D.D.C. 2020); *see also Marland*, 498 F. Supp. 3d at 637 ("the effect of the Identification will be to undermine the app's functionality such that U.S. users will be prevented from exchanging data on the app.").

The same principle applies here. Before OFAC's sanctions, which are being challenged in court in two separate lawsuits, law-abiding Americans used Tornado Cash software for legitimate privacy purposes. In *Van Loon v. Department of the Treasury*, six Americans brought

suit claiming that OFAC's sanctions unlawfully prohibited their use of Tornado Cash, which they described as "a decentralized, open-source software project that restores some privacy for Ethereum users." Complaint ¶ 4, Case No. 6:22-cv-920 (W.D. Tex. Sept. 8, 2022). Another challenge was brought by Coin Center, a U.S. nonprofit entity, and three individual Tornado Cash users who alleged that they "use Tornado Cash to protect their privacy." Complaint ¶ 21, Case No. 3:22-cv-20375 (N.D. Fla. Oct. 12, 2022). The government may not use the IEEPA to criminalize a privacy-enhancing platform any more than it could use the IEEPA to shut down a social media platform.

2. The IEEPA Charge Fails to Allege that Roman Storm Willfully Conspired to Evade Sanctions on North Korea

Count Three fails for a second reason, too. It fails to allege that Mr. Storm willfully did anything unlawful (he did not). (*See* Ind. ¶¶ 84-88); 50 U.S.C. § 1705. To establish a "willful" violation of the IEEPA or an IEEPA-promulgated regulation "the [g]overnment must prove that the defendant acted with knowledge that his conduct was unlawful." *Bryan v. United States*, 524 U.S. 184, 192 (1998) (internal quotation marks omitted); *see also United States v. Homa Int'l Trading Corp.*, 387 F.3d 144, 147 (2d Cir. 2004) (applying the *Bryan* willfulness standard to IEEPA); *United States v. Griffith*, 515 F. Supp. 3d 106, 121 (S.D.N.Y. 2021) (same).

As explained below, Count Three fails this basic prerequisite. There is no allegation of any unlawful conduct at all by Mr. Storm during the development and launch of Tornado Cash in 2020. By the time that Lazarus Group allegedly began using Tornado Cash two years later, Tornado Cash was immutable, meaning it could not be altered to prevent use by Lazarus Group or anyone else with an Internet connection. (*See* Fed Primer at 135 ("Smart contract-based protocols without privileged access [like Tornado Cash] are immutable and therefore not capable of changing their behavior by design.").) Even the Indictment concedes that Mr. Storm and other

developers relinquished control over the Tornado Cash software years earlier (Ind. ¶ 26)—and it was freely available to anyone in the world who wanted to use it. There was nothing Mr. Storm could do to prevent Lazarus Group from using it, which means he did not "have a free will or choice" with respect to the alleged IEEPA evasion efforts of Lazarus Group. *United States v. Ill. Cent. R. Co*., 303 U.S. 239, 243 (1938) (defining "willfully"); *see also Bryan*, 524 U.S. at 191 (willfulness "differentiates between deliberate and unwitting conduct."); *Smith v. Wade*, 461 U.S. 30, 73 n.8 (1983) (willfulness implies "a determination with a bad intent") (quotation omitted)).

(a) Willfulness requires allegations that a defendant made a deliberate choice to violate the law.

The IEEPA's willfulness requirement has a long history, dating back to Word War I and the passage of the Trading with the Enemy Act ("TWEA"). *See United States v. Amirnazmi*, 645 F.3d 564, 572 (3d Cir. 2011) ("IEEPA traces its provenance to § 5(b) of the Trading with the Enemy Act."). Congress added a willfulness requirement to TWEA out of concern that innocent people might be wrongly prosecuted unless the government was required to prove a deliberate and intentional choice to aid the enemies of the United States. *See* 55 Cong. Rec. 7015 (1917) ("[t]o say that a man can be held because he has merely reasonable cause to believe may be quite a dangerous thing … The inquiry I make is whether the word 'knowledge' is not sufficient …." (statements of Sen. Reed)). The solution was the addition of the word "willfully" to the statute because that term "means that a man … ***deliberately and willfully makes up his mind*** to trade with [the enemy], to commit an offense." *Id.* at 7016 (emphasis added).

Years later in 1977, Congress passed some reforms to TWEA, one of which was the enactment of the IEEPA, which contains the same willfulness requirement. *See Amirnazmi*, 645 F.3d at 572; *see also* 50 U.S.C. § 1705(c). In the context of North Korean sanctions, the government must "prove that (1) [Defendant] knowingly and willfully joined a conspiracy with

knowledge of its unlawful object, *i.e.*, the providing services to the DPRK." *Griffith*, 515 F. Supp. 3d at 120; *see also Homa Int'l Trading Corp.*, 387 F.3d at 147 (same). When the charge is conspiracy to violate the IEEPA, the willfulness inquiry must be satisfied "at the time [Defendants] joined in a plan to engage in the unlawful acts." *United States v. Quinn*, 403 F. Supp. 2d 57, 60 (D.D.C. 2005).

(b) The government has not and cannot allege that Roman Storm made a deliberate choice to violate the IEEPA.

The correct application of the willfulness requirement eviscerates the IEEPA conspiracy charge, because, throughout the time of the alleged conspiracy, there was not a single deliberate choice allegedly made by Mr. Storm to evade or to conspire to evade sanctions.

(i) The government does not even try to allege that Roman Storm developed Tornado Cash for sanctions evasion purposes.

The government alleges the conspiracy began on April 14, 2022, two years after Tornado Cash had become publicly available and immutable in May 2020 (Ind. ¶ 26), which concedes that Mr. Storm's involvement in the development or launch of Tornado Cash was *not* part of an effort to evade sanctions. The Indictment alleges no facts that would show willfulness to violate sanctions, or to assist some sanctioned person or entity to violate sanctions, at the time the Tornado Cash protocol's code was being written by Mr. Storm and the Peppersec developers and open sourced to the public. This alone vitiates any showing of willfulness.

(ii) When Lazarus Group allegedly chose to independently and publicly use Tornado Cash, there was nothing that Roman Storm could do to stop them.

The government instead fast-forwards two years and alleges the conspiracy began in April 2022, but by that time, Tornado Cash was immutable, which is further fatal to the Indictment's willfulness allegation. When Lazarus Group allegedly decided to misuse Tornado

Cash beginning on March 29, 2022, it was already available on the Ethereum blockchain for use by anyone with an Internet connection, and its code could not be changed or taken down, even by Mr. Storm himself. There is no allegation that Lazarus Group was a customer of Peppersec or made any arrangements with Mr. Storm. As with the alleged money laundering conspiracy discussed above, the Indictment faults Mr. Storm for allegedly not doing enough to stop Lazarus Group ***after*** they had already begun trying to evade sanctions.

This is overreach. The Indictment acknowledges that a sophisticated user can use the Tornado Cash protocol directly. (Ind. ¶ 13.) If Lazarus Group did use Tornado Cash, it certainly had that sophistication. Ignoring the obvious, the government insists that Lazarus Group needed help and got that help in the form of the UI. (*Id.* ¶¶ 60-68.) But even assuming that Lazarus Group did use the UI—the Indictment identifies no evidence of such use—none of these allegations shows a deliberate choice by Mr. Storm to evade North Korean sanctions.

First of all, the Indictment admits that the sanctioned Lazarus Group wallet address was in fact blocked from using Peppersec's UI, which shows compliance, not evasion. (*Id.* ¶¶ 63-64.) While the Indictment complains that this blocking was ineffective (*Id.* ¶ 65), nowhere does the Indictment allege that Mr. Storm willfully chose to refrain from blocking any other known wallet addresses allegedly used by Lazarus Group.

Additionally, the Indictment alleges that Mr. Storm should have shut down the entire UI. (*Id.* ¶¶ 67-68.) But the web hosting fee associated with the UI was plainly not for the benefit of Lazarus Group, since the UI was maintained to make Tornado Cash accessible to unsophisticated users (*id.* ¶ 13)—*i.e.*, users other than Lazarus Group. Moreover, shutting down the UI would not have prevented Lazarus Group from continuing its alleged misuse of Tornado Cash by directly accessing its smart contracts on the public Ethereum blockchain. Indeed, and notably,

the government itself took no steps to demand that the UI be taken down by Mr. Storm or by the U.S.-based web service that hosted it. (*Id.* ¶ 14.)

Finally, to the extent the Indicment relies on cherry-picked sentences from Mr. Storm's purported chats, they do not show willfulness either. (*See* Section IV.B.2.b *supra*.) The alleged statements by Mr. Storm and others expressing surprise or fear of potential legal or reputational exposure, after the Indictment alleges bad actors independently used the Tornado Cash smart contracts, do not show a conspiracy or a willful attempt to evade sanctions.

(iii) The government's own allegations confirm that Roman Storm did not willfully attempt to evade sanctions.

Even if the government could prove every single one of the Indictment's deficient allegations, it would not establish an IEEPA violation. Mr. Storm's lack of willfulness becomes clear when the government's allegations here are compared to other IEEPA cases.

Mr. Storm did not express a desire to help Lazarus Group. The typical IEEPA case features an allegation that the defendant desired to transact with a sanctioned person. *See, e.g.*, *Griffith*, 515 F. Supp. 3d at 121 ("The government represents that it will offer evidence that Griffith expressed a desire to return to the DPRK and help them utilize cryptocurrency");[25] *Sarvestani v. United States*, 2015 WL 7587359, at *3 (S.D.N.Y. Nov. 25, 2015) (Defendant admitted "he had conspired with another person to sell American–made goods to Iran … that he knew 'at the time' that his conduct violated U.S. law"). Mr. Storm is not even alleged to have done that with respect to Lazarus Group or North Korea.

[25] The *Griffith* case is also distinguishable because it turned on Judge Castel's conclusion that only *pre-existing* materials qualify for the informational materials exemption. 515 F. Supp. at 116. That argument is inapposite because the Tornado Cash software was developed, published, and in existence two years before the alleged sanctions evasion conspiracy began in April 2022.

Mr. Storm did not try to conceal Lazarus Group's alleged misconduct. The Indictment does not allege that Mr. Storm tried to conceal the misuse of Tornado Cash or lie about who was using it. *Cf. United States v. Kuyumcu*, 2017 WL 3995576, at *5-6 (E.D.N.Y. Sep. 8, 2017) (defendant knew of the export restrictions and lied about end users). Nor does it allege that Mr. Storm tried to alter any transaction records or create fraudulent records to obscure transactions. *Cf. United States v. Shavkat Abdullaev*, 761 F. App'x 78, 81-82 (2d Cir. 2019) (defendant "prepared fraudulent documentation for each charged export.").

Mr. Storm did not attempt to deceive the government. The Indictment fails to allege that Mr. Storm did anything to deceive the government or impede its investigation. *Cf. Homa Int'l Trading Corp.*, 387 F.3d at 147 (defendant conducted "clandestine transactions" even after receiving letters from OFAC); *United States. v. Halkbank*, No. 15 CR 867 (RMB), 2020 WL 6273887, at *1 (S.D.N.Y. Oct. 26, 2020) (involving complex sanctions evasion scheme, including lying to Treasury officials).

Mr. Storm tried to block the sanctioned Lazarus Group wallet. The Indictment admits that Mr. Storm changed the Tornado Cash UI "to block deposits directly from OFAC-designated addresses," which is the opposite of sanctions evasion. (Ind. ¶ 64; *cf. United States v. Nejad*, No. 18-cr-224 (AJN), 2019 WL 6702361, at *1 (S.D.N.Y. Dec. 6, 2019) (defendant evaded sanctions by continuing to make payments through a web of defendant-controlled entities).)

Mr. Storm had no arrangement to be compensated by Lazarus Group. The Indictment concedes that Mr. Storm was not compensated by Lazarus Group. This is a significant concession considering the unlikelihood of anyone agreeing to take on the risk of sanctions evasion without substantial compensation. *Cf. Banki,* 685 F.3d at 104 (defendant was paid almost $3.4 million for facilitating illicit transfers of funds from Iran to U.S.); *United States v.*

Atilla, 966 F.3d 118, 122 (2d Cir. 2020) (part of sanctions evasion scheme included payment of "millions of dollars in bribes to other codefendants").

In short, Count Three represents prosecutorial overreach untethered from established IEEPA law. The Second Circuit has repeatedly observed that "a conspiracy by its very nature is a secretive operation." *Jackson*, 335 F.3d at 180. Here, by contrast, the alleged conspiracy took place using public software available on the public Ethereum blockchain, which publicly documented the transactions at issue permanently for viewing by the government and anyone else who cares to look. No one would willfully publicize the key details of a sanctions-evasion conspiracy or willfully carry it out without an agreement to be compensated by the persons seeking to evade sanctions. Count Three is fatally deficient and should be dismissed.

D. All Counts Should Be Dismissed on First Amendment Grounds

The charges against Mr. Storm should be dismissed on First Amendment grounds. As a threshold matter, the protections of the First Amendment apply to computer code, and computer programs constructed from code. *See, e.g., Corley*, 273 F.3d at 449; *Junger v. Daley*, 209 F.3d 481, 485 (6th Cir. 2000) ("Because computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment."). Further, "[i]t is well-established that First Amendment rights may be violated by the chilling effect of governmental action that falls short of a direct prohibition against speech." *Zieper v. Metzinger*, 474 F.3d 60, 65 (2d Cir. 2007). The statutes violate the First Amendment both because they are overbroad and because they do not survive strict scrutiny as applied to Mr. Storm's alleged conduct.

1. The Statutes Are Unconstitutionally Overbroad

All three statutes underlying the conspiracy charges are unconstitutionally overbroad. "The purpose of an overbreadth challenge is to prevent the chilling of constitutionally protected conduct, as prudent citizens will avoid behavior that *may* fall within the scope of a prohibition, even if they are not entirely sure whether it does." *Farrell v. Burke*, 449 F.3d 470, 499 (2d Cir. 2006). In conducting an overbreadth analysis, the Court determines whether the statute, as construed, "criminalizes a substantial amount of protected expressive activity." *United States v. Williams*, 553 U.S. 285, 297 (2008).

Here, the statutes underlying the conspiracy charges, as construed by the government, are facially overbroad. Specifically, Count One alleges a conspiracy to commit money laundering by defining a "financial institution" to include the Tornado Cash smart contracts—software programs over which defendant had no control since at least May 2020, as the Indictment concedes—and by including, within the statutory definition of "conducting" a financial transaction, the mere writing and/or dissemination of the code for those smart contracts. (*See* Section IV.B.1 *supra*.) Count Two similarly alleges a conspiracy to operate an unlicensed money transmitting business by defining Tornado Cash as a money transmitting business and by alleging that the mere writing and/or dissemination of the smart contracts that operate the Tornado Cash pools constitute involvement in the "transmission" of funds, notwithstanding FinCEN guidance to the contrary. (*See* Section IV.A *supra*.) Count Three fares no better, alleging a conspiracy to evade sanctions for merely maintaining a website providing the public information to access the Tornado Cash smart contracts, notwithstanding the statute's broad exception for informational materials. (*See* Section IV.C.1 *supra*.) All three statutes are therefore unconstitutionally overbroad insofar as they criminalize: (1) the writing and

dissemination of computer code designed to improve the privacy of personal financial transactions; or (2) the maintenance of websites publishing such code.

Not only is computer code protected by the First Amendment, but privacy over financial transactions is itself a constitutionally protected interest. *Statharos v. N.Y. City Taxi & Limousine Comm'n*, 198 F.3d 317, 322–23 (2d Cir. 1999) ("[T]his Court has recognized the existence of a constitutionally protected interest in the confidentiality of personal financial information."). As a result, the statutes have a substantial chilling effect on the First Amendment rights of computer programmers who seek to create and publish computer code that improves privacy over an individual's financial transactions, whether they are communicating with users of the program or with other programmers. *See Corley*, 273 F.3d at 449 (identifying three ways "in which a programmer might be said to communicate through code: to the user of the program"; "to the computer"; and "to another programmer"). To the extent these statutes criminalize and chill legitimate expressive activity—the publication of computer code supporting a constitutionally protected interest—they are unconstitutionally overbroad, and all three conspiracy charges premised on them should be dismissed.

2. The Statutes Violate the First Amendment As Applied

Even assuming the statutes are not facially overbroad, all three conspiracy charges should be dismissed because the statutes, as applied, violate the First Amendment.[26] In the context of criminal statutes, more careful scrutiny is required. *See Holder v. Humanitarian Law Project*,

[26] Although as-applied challenges may be considered premature on a motion to dismiss where there is a need for a "full factual development at trial" before a court can determine whether the "statutes failed to provide defendant fair warning that his conduct was prohibited by law," *United States v. Phillips*, No. 22-CR-138 (LJL), 2023 WL 5671227, at *13 (S.D.N.Y. Sept. 1, 2023), there is no need for further factual development here as the factual allegations in the Indictment are sufficient to demonstrate the unconstitutionality of the statutes as applied.

561 U.S. 1, 28 (2010) (applying more rigorous scrutiny to criminal laws); *City of Hous., Tex. v. Hill*, 482 U.S. 451, 459, (1987) ("Criminal statutes must be scrutinized with particular care."). The scope of the First Amendment's protections depend on whether the restrictions are imposed because of the content of the speech. *Corley*, 273 F.3d at 450. "Government regulation of speech is content based if a law applies to particular speech because of the topic discussed or the idea or message expressed." *Reed v. Town of Gilbert, Ariz.*, 576 U.S. 155, 163 (2015).

(a) Strict Scrutiny Applies to the Content-Based Regulations Here.

Content-based restrictions are subject to strict scrutiny. *Reed*, 576 U.S. at 163 ("Content-based laws—those that target speech based on its communicative content—are presumptively unconstitutional and may be justified only if the government proves that they are narrowly tailored to serve compelling state interests."); *see also Corley*, 273 F.3d at 450 ("Content-based restrictions are permissible only if they serve compelling state interests and do so by the least restrictive means available.").

Here, the statutes underlying the conspiracy charges are, as applied, content-based regulations of constitutionally protected speech and are therefore subject to strict scrutiny. The Indictment alleges a conspiracy to violate three statutes based on the writing and dissemination of computer code that allows users to improve privacy protections for financial transactions on the Ethereum blockchain, as well as the maintenance of a website providing access to and information about such code, without any involvement in the underlying transactions. The government's regulation of the speech here is clearly content-based, as it both: (1) targets the function or purpose of the speech; and (2) cannot be justified without reference to the content of the regulated speech—computer code designed to improve the privacy of personal financial transactions, which, again, is a constitutionally protected interest. *Statharos*, 198 F.3d at 322–23. It has also arguably been adopted "because of disagreement with the message [the speech]

conveys," *Reed*, 576 U.S. at 164, since the Indictment is littered with suggestions that there is no legitimate purpose for maintaining privacy over one's financial transactions on an otherwise completely transparent and publicly viewable blockchain. (*See, e.g.*, Ind. ¶¶ 9-11, 35.) Because the government's application of the statutes here is content-based, strict scrutiny should apply.[27]

(b) The Statutes, As Applied, Do Not Survive Strict Scrutiny.

The government's application of the statutes at issue here cannot withstand strict scrutiny.[28] As a threshold matter, the government has the burden of proving that its regulation withstands First Amendment scrutiny. *See, e.g., Edenfield v. Fane*, 507 U.S. 761, 770 (1993). The government cannot meet its burden here because the statutes, as applied, are not the least restrictive means of serving the government's interests in preventing money laundering (Count One); in regulating money transmitting businesses (Count Two); and in enforcing sanctions (Count Three), even assuming these are "compelling" state interests. As the Indictment acknowledges, the Tornado Cash Compliance Tool allowed users "to document their own transaction history if they chose to do so." (Ind. ¶ 39.) Rather than criminalize attempts to improve privacy in transactions conducted on the Ethereum blockchain, the government could, for example, require individuals and entities that conduct transactions in ETH to collect

[27] To the extent the government's regulation applies to the website hosting the version of the UI Peppersec created, the regulation of websites containing "images, words, symbols, and other modes of expression" should be protected under the First Amendment as "pure speech." *See 303 Creative LLC v. Elenis*, 600 U.S. 570, 587 (2023).

[28] Even assuming the statutes are being applied in a content-neutral manner, they still fail to withstand First Amendment scrutiny because they are not narrowly tailored to achieve the government's interests, for the same reasons set forth herein. *See Cornelio v. Conn.*, 32 F.4th 160, 171 (2d Cir. 2022) ("The burden of demonstrating that the [regulation at issue] satisfies intermediate scrutiny falls on the government. To carry that burden, the government must show that the challenged law (1) advances important governmental interests unrelated to the suppression of free speech and (2) does not burden substantially more speech than necessary to further those interests.") (citations omitted).

documentation proving the source of funds from any customer seeking to transfer or convert ETH that has been previously withdrawn from Tornado Cash (or similar application). Because there are less restrictive means for the government to achieve its goals, the Indictment's three counts should be dismissed on First Amendment grounds.

E. All Counts Should Be Dismissed on Due Process Grounds

The statutes underlying Mr. Storm's charges did not put him on fair notice that his alleged conduct violated the law. The Due Process right to fair notice, or "fair warning," manifests itself in three ways: (1) the vagueness doctrine; (2) the rule of lenity; and (3) the bar on novel constructions of a criminal statute. *See United States v. Lanier*, 520 U.S. 259, 266 (1997). The statutes at issue here violate all three, and the charges against Mr. Storm must be dismissed.

1. The Statutes Are Void for Vagueness

A statute is unconstitutionally vague under the Due Process Clause if it "fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement." *Williams*, 553 U.S. at 304. "The degree of vagueness tolerated in a statute varies with its type: economic regulations are subject to a relaxed vagueness test, laws with criminal penalties to a stricter one, and laws that might infringe constitutional rights to the strictest of all." *Rubin v. Garvin*, 544 F.3d 461, 467 (2d Cir. 2008).

(a) <u>The statutes are facially vague.</u>

"A vagueness challenge to a statute may be facial—a claim that the law is invalid *in toto*, incapable of any valid application—or as-applied." *Bastian*, 112 F. Supp. 2d at 380. Facial vagueness challenges may be brought where a statute "reaches 'a substantial amount of constitutionally protected conduct,' particularly rights protected by the First Amendment."

Copeland v. Vance, 893 F.3d 101, 111 (2d Cir. 2018) (quoting *Kolender v. Lawson*, 461 U.S. 352, 358 n.8 (1983)). But "all vagueness challenges—whether facial or as-applied—require us to answer two separate questions: whether the statute gives adequate notice, and whether it creates a threat of arbitrary enforcement." *Farrell*, 449 F.3d at 485. For facial challenges, courts "must consider not only conduct clearly prohibited by the regulation but also conduct that arguably falls within its ambiguous sweep." *Id.* at 499. "[W]here a statute imposes criminal penalties, the standard of certainty is higher." *Kolender*, 461 U.S. at 358 n.8.

As discussed above, it is well established that the First Amendment protects software code as speech. (*See* Section IV.D *supra*.) Thus, the statutes underlying the conspiracy charges against Mr. Storm seek to criminalize expression protected by the First Amendment and are subject to facial vagueness challenges. *Parker v. Levy*, 417 U.S. 733, 759 (1974). The Indictment alleges that Mr. Storm's publication of software code, without any direct involvement in the actual transactions proscribed by the underlying statutes, supports charges of conspiracy to violate those statutes. (*See* Ind. ¶¶ 77-88.) This unprecedented and novel application underscores the unconstitutionally vague nature of those statutes. Under the government's theory, all three statutes criminalize the publication of *any* software that may later be misused by a third party, even where the author of such code is not involved in or even aware of such misuse. In the case of *immutable* software programs—which, like the Tornado Cash smart contracts at issue at here, cannot be modified or deleted once published—the author of such code would require an extremely high level of confidence that there is no possibility of misuse prior to disseminating the code. Thus, by including within their respective ambits the mere writing and publication of computer code with a legitimate, lawful function that may nevertheless be misused by a third party subsequent to its release, the statutes fail to provide fair notice to computer

programmers and others seeking to write and disseminate code for public use. Specifically, the statutory definitions of: (1) a "financial transaction" under 18 U.S.C. § 1956 (Count One); (2) "accepting" and "transmitting" under 18 U.S.C. § 1960 (Count Two); and (3) "informational materials" under 50 U.S.C. § 1702(b)(3) are all facially vague, as they would not put a person of ordinary intelligence on notice that the publication of code, without any involvement in underlying transactions, would fall within the proscriptions of the statutes.

Further, the statutes also invite arbitrary enforcement because there are no explicit standards for their application. Without explicit standards that govern when a writer of code is: (1) conducting a "financial transaction"; (2) "accepting" and "transmitting" funds; or (3) providing "informational materials," it is unclear whether the mere dissemination of the code is sufficient to violate the statutes or whether the author must maintain a website or some other repository where information regarding the code is made available to potential users—both of which involve legitimate expressive activity. It is also unclear whether the statutes extend only to the writing and dissemination of code over which the author retains control or whether they extend to immutable code, subjecting the author to criminal liability for a third party's misuse that the author did not anticipate. The statutes are thus facially vague, and the charges based on them should be dismissed.

(b) The statutes are vague as applied.

The statutes are also unconstitutionally vague as applied here. The same two-part test applies for an as-applied challenge, but the focus is on the defendant's conduct. *See Farrell*, 449 F.3d at 485. For the same reasons set forth above, all three of the underlying statutes fail under this two-part test. An ordinary person of reasonable intelligence would not know that, by merely writing and disseminating computer software code that seeks to improve privacy over personal

financial transactions, that person may be found criminally liable under 18 U.S.C. § 1956, 18 U.S.C. § 1960, or 50 U.S.C. § 1702(b)(3). And for the same reasons discussed above, there are no explicit standards for those who apply it. Because all three statutes are unconstitutionally vague as applied here, the Indictment must be dismissed.

2. All Counts Should Be Dismissed Pursuant to the Rule of Lenity

The rule of lenity, when considered in conjunction with the arguments raised above, also mandates that all three counts be dismissed. "[A]mbiguity concerning the ambit of criminal statutes should be resolved in favor of lenity." *Rewis v. United States*, 401 U.S. 808, 812 (1971) (citations omitted). The rule "is premised on two ideas: First, a fair warning should be given to the world in language that the common world will understand, of what the law intends to do if a certain line is passed; second, legislatures and not courts should define criminal activity." *Babbit v. Sweet Home Chapter of Communities for a Great Oregon*, 515 U.S. 687, 704 n.18 (1995) (citations and internal quotations omitted). The Indictment alleges a novel and expansive interpretation of the statutes underlying the conspiracy charges, as has been fully detailed above. Expanding criminal liability to the alleged conduct would involve a "sweeping expansion of federal criminal jurisdiction in the absence of a clear statement by Congress" in violation of the rule of lenity. *See Cleveland v. United States*, 531 U.S. 12, 24 (2000); *see also Banki*, 685 F.3d at 109 (applying rule in vacating convictions for violating Iran sanctions and explaining that "[t]he rule of lenity requires ambiguous criminal laws to be interpreted in favor of the defendants subjected to them"). As such, all three counts should be dismissed pursuant to the rule of lenity.

3. All Counts Should Be Dismissed as Novel Constructions

Finally, all three counts should be dismissed under the Due Process clause because, for all of the reasons set forth above, the Indictment impermissibly relies upon a "novel construction

of a criminal statute to conduct that neither the statute nor any prior judicial decision has fairly disclosed to be within its scope." *Lanier*, 520 U.S. at 266. In adopting such an expansive interpretation of the statutes, the government is creating a constitutional issue where none need exist, as the statutes are clearly meant to apply to persons and entities with more substantial involvement in the underlying transaction(s). *See Clark v. Martinez*, 543 U.S. 371, 380-81 (2005) ("[W]hen deciding which of two plausible statutory constructions to adopt, a court must consider the necessary consequences of its choice. If one of them would raise a multitude of constitutional problems, the other should prevail—whether or not those constitutional problems pertain to the particular litigant before the Court.").

There is simply no precedent for the expansive application of the statutes to Mr. Storm's conduct as alleged in the Indictment, and the Court should not entertain such a novel construction now. Counsel, not surprisingly, have found no judicial decisions holding that the constitutionally protected activity of providing code to users who wish to protect their financial privacy can constitute money laundering, operating a money transmitting business, or evading sanctions. The Court should therefore adopt a limiting construction of each of the statutes charged here to preclude enforcement based on the allegations contained in the Indictment. Only by so limiting the reach of the statutes can they be given their proper meaning and a meaning that avoids the constitutional problems identified above.

V. CONCLUSION

For all the reasons above, the Court should dismiss the Indictment against Mr. Storm in its entirety with prejudice.

Dated: March 29, 2024

Respectfully submitted,

/s/ Brian E. Klein

Brian E. Klein
Keri Curtis Axel
Kevin M. Casey
Waymaker LLP

Attorneys for Roman Storm